IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	
	)	**No. 18 CR 789**
v.	)	
	)	**Hon. Gary Feinerman**
DENY MITROVICH,	)	
	)	
Defendants.	)	

REPLY IN SUPPORT OF HIS MOTION TO COMPEL DISCOVERY

Now comes the defendant, Deny Mitrovich, by and through his undersigned attorney, and respectfully submits the following reply in support of his motion to compel discovery:

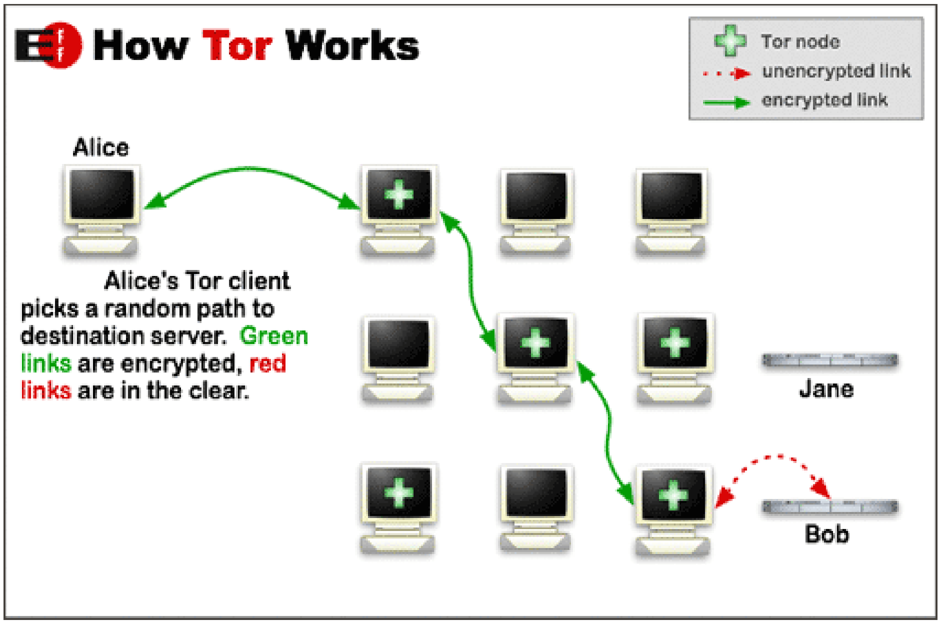
Mr. Mitrovich did not voluntarily disclose his IP address, or a session identifier, to the QPS/DIA when he clicked on the hyperlink that redirected him from the Tor Browser to the open internet because in order to do so a malicious code (or "malware") had to be installed on his computer, which, without a warrant, constitutes a Fourth Amendment violation. Essentially, because of the way the Tor Network and Tor Browser operates, the hyperlink must have contained malware that forced Mr. Mitrovich's computer to send the identifying information to QPS/DIA or forced it to exit from the Tor Browser and onto the open internet. It would have been impossible to do so otherwise. Even the government implies that some sort of malware was used to obtain the information because if the hyperlink was just that, a hyperlink, there would be no source code to refuse disclosing. Further, this technique has been used repeatedly by the FBI in similar watering hole, sting-like operations to identify users of elicit hidden services on the Tor Network. Mr. Mitrovich's case parallels these cases where the FBI admitted to having used malware and, as such, sought a warrant. This also raises the question that if identifying a Tor user's IP address is as simple as posting a hyperlink that redirects to the open internet without trespassing a user's computer with malware, why would the government not always use this method instead of applying for warrants as they do in all other similar matters?

Courts that have addressed the malware issue relating to watering hole operations have determined that the malware engaged in a Fourth Amendment search. Even though one may not have had a reasonable expectation of privacy in some of the information on the computer, the courts held that a person does have a broader expectation in the computer itself through, at least in part, the Fourth Amendment property-based approach. Thus, the government had to obtain a warrant in order to lawfully deploy their malware into Mr. Mitrovich's computer. This Court must order the government to disclose the source code used to send malware into Mr. Mitrovich's computer and any and all correspondence between them and QPS/DIA in order for Mr. Mitrovich to be able to be able to effectively litigate a motion to suppress.

In determining whether to compel the government to disclose this requested information, this Court must weight Mr. Mitrovich's rights under the constitutionally guaranteed Fourth Amendment protections against the government's interest in not disclosing how they investigated Mr. Mitrovich. It simply does not follow that the government is able to utilize increasingly invasive technology without allowing the accused to determine whether or not their rights were violated. Without access to this software and source code, Mr. Mitrovich will simply have to live – in prison – with the fact that the government may have encroached on his constitutional rights without any recourse or ability to even see if they did. This is not right.

I. How the Tor Network and Tor Browsing Works

The Tor Network is a system of relays which tunnels a user's internet activity through the Tor Network while masking the user's IP address and physical location and at the same time encrypting the data. The following diagram[1] from the Tor Project illustrates how Tor operates:


How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

In the illustration, for purposes of this submission, let us presume that Mr. Mitrovich is Alice, the Tor user, and The Love Zone website ("TLZ"), is Bob. The first computer with a plus sign that Alice connects to is called the entry node. When Alice connects to the Tor Network, all of her online traffic gets tunneled to the entry node and is

[1] Image from Tor: Overview, The Tor Project *available at* https://2019.www.torproject.org/about/overview.html.en (last accessed Jan. 28, 2020).

encrypted as it is sent. At this point, the entry node knows the IP address of Alice's computer but cannot see data that is sent from Alice's computer. The entry node then adds another layer of encryption and sends the traffic to another relay (the second computer with a plus sign). The second relay does not see Alice's IP address and cannot read any of the data that is sent. The relay then adds a third layer of encryption and sends the computer connection to the exit node (the third computer with a plus sign). The exit node does not see Alice's IP address or the IP address of the entry node. It only knows the IP address of the relay that sent Alice's, now thrice, encrypted data.[2]

In order to access the Tor Network, a user must download certain software (a browser), the most common of which was developed by the Tor Project itself—the Tor Browser. As this Court knows, certain computer applications and functions automatically connect to servers on the open internet which can potentially lead to identity leaks, such as IP address leaks, because that specific traffic is not sent through the Tor Network. The Tor Browser addresses these potential identity and IP address leaks by disabling the applications and functions that connect to the open internet.[3] As such, Mr. Mitrovich's computer could not have been leaking its identity

[2] For general overview, *see* Tor Overview, The Tor Project, *available at* https://2019.www.torproject.org/about/overview.html.en (last accessed Jan. 28 2020).

[3] *See* FAQ: So I'm Totally Anonymous If I Use Tor?, The Tor Project *available at* https://2019.www.torproject.org/docs/faq.html.en#AmITotallyAnonymous (explaining that certain applications like Javascript and Adobe Flash may have the ability to ignore proxy settings due to their permissions given in the operating system. The Tor Browser, however, addresses the potential identity leaks associated with these applications: "That's where Tor Browser comes in. We produce a web browser that is preconfigured to help you control the risks to your privacy and anonymity while browsing the Internet. Not only are the above technologies disabled to prevent identity leaks, Tor

information and its IP address through these functions because, otherwise, there would have been no need to have Mr. Mitrovich click on the infected hyperlink—had his computer been leaking his IP address, then servers on the open internet would already be capturing his identity.[4] Additionally, if the Tor Browser in genreal was leaking IP address on its own, then the government would not have needed to use malware in past watering hole operations. This is why it was necessary for the government to use the malware-embedded hyperlink in this sting-like investigation.

While connected to the Tor Network – through the Tor Browser – any website that Alice, or in this case Mr. Mitrovich, visits is tunneled through the Tor network and goes through its respective relays. It does not matter if the website is on the open internet,[5] like Facebook or YouTube, or a website that is a hidden service only accessible through the Tor Network—all traffic from Alice's computer is tunneled through the Tor Network.[6] Tor is specifically marketed as a way for individuals to get

Browser also includes browser extensions like NoScript and Torbutton, as well as patches to the FireFox source code.") (last accessed Jan. 28, 2020).

[4] *See also* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired, (Sept. 13, 2013), https://www.wired.com/2013/09/freedom-hosting-fbi/ (explaining that the government malware used in the Freedom Hosting operation, as discussed *infra*, was a Javascript code that exploited a vulnerability in the Tor Browser forcing computers to send identifying information through the open internet (the data was sent "as a standard HTTP web request."). This shows that certain functions, like Javascript, can leak identifying information, the Tor Browser, however, is configured to prevent the computer from doing so on its own) (last accessed Jan. 28, 2020).

[5] *See*, *e.g.* Tor Browser Manuel: Managing Identities, The Tor Project *available at* https://tb-manual.torproject.org/managing-identities/ (explaining that browsing the open internet with a non-Tor browser allows the website and third-party services to track information about the visiting user, including location information. It further explains that using the Tor Browser on the Tor Network "stops observers from being able to discover your exact location and IP address" which means that users can visit the same sites on the public internet while still preventing the website or third-party services from seeing the user's IP address) (last accessed Jan. 28, 2020).

[6] *See* FAQ: What Protections Does Tor Provide?, The Tor Project *available at* https://2019.www.torproject.org/docs/faq.html.en#WhatProtectionsDoesTorProvide ("Generally

around government censorship and explicitly states "if you can get to any part of the Tor Network, you can reach any site on the Internet."[7] Therefore, as long as Alice is browsing the internet through the Tor Browser, the only IP address that an open internet site, like YouTube, can see is the IP address of the exit node.[8] In fact, the

speaking, Tor aims to solve three privacy problems: First, Tor prevents websites and other services from learning your location, which they can use to build databases about your habits and interest. With Tor, your Internet connections don't give you away by default – now you can have the ability to choose, for each connection, how much information to reveal. Second, Tor prevents people from watching your traffic locally (such as your ISP or someone with access to your home wifi or router) from learning what information you're fetching and where you're fetching it from. It also stops them from deciding what you're allowed to learn and publish – if you can get to any part of the Tor network, you can reach any site on the Internet. Third, Tor routes your connection through more than one Tor relay so no single rely can learn what you're up to. Because these relays are run by different individuals or organizations, distributing trust provides more security than the old one hop proxy server.") (last accessed Jan. 28, 2020) ; *see also* FAQ: So I'm Totally Anonymous If I Use Tor?, The Tor Project *available at* https://2019.www.torproject.org/docs/faq.html.en#AmITotallyAnonymous ("First, Tor protects the network communications. It separates where you are from where you are going on the Internet. What content and data you transmit over Tor is controlled by you. If you login to Google or Facebook via Tor, the local ISP or network provider doesn't know you are visiting Google or Facebook. Google and Facebook don't know where you are in the world. However, since you have logged into their sites [using your personal login information], they know who you are.") (last accessed Jan. 28, 2020).

[7] *See*, footnote 6, FAQ: What Protections Does Tor Provide?

[8] *See* Tor Browser Manuel: About Tor Browser, The Tor Project *available at* https://tb-manual.torproject.org/about/ ("Tor Browser uses the Tor network to protect your privacy and anonymity. Using the Tor network has two main properties: [First] Your internet service provider, and anyone watching your connection locally, will not be able to track your internet activity, including the names and address of the websites you visit. [Second] The operators of the websites and services that you use, and anyone watching them, will see a connection coming from the Tor network instead of your real Internet IP address, and will not know who you are unless you explicitly identify yourself…Tor is a network of virtual tunnels that allows you to improve your privacy and security on the Internet. Tor works by sending your traffic through three random servers (also known as *relays*) in the Tor network. The last relay in the circuit (the "exit relay") then sends the traffic out onto the public Internet.") (last accessed Jan. 28, 2020); *see also* Tor Overview, The Tor Project, *available at* https://2019.www.torproject.org/about/overview.html.en ("To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way only knows which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through. Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the Tor network. Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination.") (last accessed Jan. 28, 2020).

exit node does not even know Alice's IP address. For these reasons, the hyperlink that was allegedly clicked by Mr. Mitrovich could not simply have been, unbeknownst to him, a hyperlink to an open internet site. If it were, then the open internet video link would have opened within the Tor Browser and the only IP address that the open internet site could gather would have been that of the exit node.

The government simply would not be able to determine Mr. Mitrovich's IP address from any information that the exit node sent to the open internet site on its own. Instead, the hyperlink and subsequent error message must have installed some sort of malware on his device which caused his computer to send either his IP address and other identifying data, or, redirect his computer from the Tor Browser to an open internet supported browser. The hyperlink that Mr. Mitrovich alleged clicked on in this matter prompted an error message to appear prior to him being redirected to the open internet. As this Court will see, *infra*, in prior government investigations, it is precisely this sort of error message that is embedded with the malware that ultimately invades an individual's computer.

II. Similar Use of Malware in Past Government Investigations

The government has conducted similar sting-like operations targeting child pornography hidden services in the past wherein they used malware to identify the site's users. The three most publicized operations are the Operation Torpedo, Playpen and Freedom Hosting watering hole stings.[9] In all of these operations, the FBI gained

[9] These type of sting-like operations are referred to as watering hole operations. They are all conducted in the same manner: a government identifies the location of a hidden service on the Tor Network whereupon the discovery of such is sent to the government in which the server hosting the site is located. That government then takes control of the server and continues to operate the site. Once it

control of a server hosting an illicitly hidden service on the Tor Network and ultimately continued to operate the website while uploading malware to identify users. In turn, these operations led to criminal charges being brought against the websites' users. This has led to numerous district courts addressing issues arising from the use of malware and whether its use constituted a Fourth Amendment search.[10] There are also publicly disclosed documents regarding a piece of malware—CIPAV— that the FBI[11] used to identifying a bombing suspect, among others, that shares indistinguishable similarities with the software the QPS/DIA used in Mr. Mitrovich's matter. These cases, along with the publicly disclosed documents, convincingly suggests that QPS/DIA installed malware on Mr. Mitrovich's computer.

has gained control of the server, it uploads malware onto the server and forces any computer accessing the site to download the software onto their computer. The malware then forces the computer to send identifying data and information, such as an IP address and session identifier, back to a government server over the open internet. The government then uses that information to subpoena Internet Service Providers to learn the name and physical location of computer's owner. *See*, e.g., Kim Zetter, *Everything We Know About How the FBI Hacks People*, Wired, (June 15, 2016), https://www.wired.com/2016/05/history-fbis-hacking/ (last accessed Jan. 28, 2020); *and* Watering Hole Attack, Wikipedia *available at* https://en.wikipedia.org/wiki/Watering_hole_attack (last accessed Jan. 28, 2020).

[10] Almost all of the malware/watering hole cases are district court decisions and there is little, if any, Circuit court decisions addressing the matter. The Tenth Circuit issued a decision on an appeal from one of the malware district court decisions, but it did not directly address whether the use of the NIT malware was a search. Instead it focused on whether a Rule 41 violation warranted suppression (as discussed below, one of the main arguments asserted by defendants in NIT cases was that the single warrants authorizing NIT's use violated the jurisdiction requirements of Rule 41 which is no longer applicable after Congress amended Rule 41's jurisdictional requirements). However, the Tenth Circuit did uphold suppression of the evidence seized by the NIT malware for violating Rule 41. *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015).

[11] CIPAV is short for "Computer And Internet Protocol Address Verifier" and it targeted web browser vulnerabilities which allowed the FBI to obtain: a computer's IP address; MAC address; open ports; a list of running programs; the operating system type, version and serial number; registered own; and list of last visited websites. *See* Kevin Poulsen, *Documents: FBI Spyware Has Been Snaring Exortionists, Hackers for Years*, Wired (May 16, 2009), https://www.wired.com/2009/04/fbi-spyware-pro/ (last accessed Jan. 28, 2020).

While the details of the specific government malware that was used in these operations is not publicly known, the government in those cases sought warrants to authorize its use in which it identified the malware as a "Network Investigative Technique" (NIT). *See*, e.g., *United States v. Knowles*, 207 F.Supp.3d 585, 589 (D.S.C. Sept. 14, 2017). These cases reveal that the malware sought the same information that was obtained from Mr. Mitrovich: his IP address and a session identifier.[12] *See United States v. Broy*, 209 F.Supp.3d 1045, 1049 (C.D. Ill. Sept. 21, 2016) (the warrant authorized NIT to obtain "the IP address of the computer…a unique session identifier generated by the NIT to distinguish data from one activating computer from that of another"); *United States v. Knowles*, 207 F.Supp.3d 585, 592-93 (D. S.C. Sept. 9, 2016) ("The NIT would 'augment' the normal content Playpen sends to users with 'additional computer instructions' that 'are designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government." The information included "the user's IP address…[and] a unique identifier generated by the NIT to distinguish data from the computer from data sent by other computers connecting to Playpen").[13]

[12] The NIT malware itself produces a "unique identifier" that allows the government the government to "distinguish data from one activating computer from that of another." *United States v. Broy*, 209 F.Supp.3d 1045, 1049 (C.D. Ill. Sept. 21, 2016). It essentially works like a serial number: the NIT would produce a unique identifier for each user that downloaded the malware so that the FBI could distinguish the users from each other and tie their activity to the hidden service. The "session identifier" obtained from Mr. Mitrovich appears to be the exact same thing as the "unique identifier" generated by NIT which strongly suggests some sort of malware was used.

[13] The following cases have all state that NIT sought IP address and generated a unique identifier, in almost the exact same language. *United States v. Owens* 2016 WL 7053195 (E.D. Wis. Dec. 5, 2016); *United States v. Workman*, 205 F.Supp.3d 1256 (D. Co. Sept. 6, 2016); *United States v. Torres*, No. 5:16-CR-28-DAE, 2016 WL 4821223, W.D. Tex. Sept. 9, 2016); *United States v. Croghan*, 209 F.Supp.3d 1080 (S.D. Iowa Sept. 22, 2016); *United States v. Anzalone*, 208 F.Supp.3d 358 (D. Mass. Sept. 22, 2016); *United States v. Dzwonczyk*, No. 4:15-CR-3134, 2016 WL 7428390 (N. Neb. Dec. 23, 2016).

The malware in those was also delivered in similar ways to how Mr. Mitrovhich's appears to have been. After the FBI gained control over the Freedom Hosting server, an error message began appearing on the hidden services page when users tried to access the website. The error message actually contained government malware which was installed on the users' computers to send the users' computer's identifying information to an FBI-controlled server in Virginia.[14] As previously stated, in 2007, the FBI used CIPAV to identify a bomb threat suspect who was anonymizing himself online. There, FBI agents posed as fake journalists and sent the suspect a MySpace message containing a hyperlink, which actually contained CIPAV. When the suspect clicked the link, CIPAV downloaded to his computer.[15] Once downloaded, "the CIPAV may cause any computer – wherever located – that activates any CIPAV authorized by the Court, (an 'activating computer') to send network level messages containing the activating computers IP address and/or MAC addresses, other environment variables, and certain registry-type information to a computer controlled by the FBI."[16] While the government has attempted to distinguish between

[14] Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired, (Sept. 13, 2013), https://www.wired.com/2013/09/freedom-hosting-fbi/ (last accessed Jan. 28, 2020).

[15] Mike Carter, *FBI Created Fake Seattle Times Web Page to Nab Bomb-Threat Suspect*, The Seattle Time (Oct. 27, 2014), https://www.seattletimes.com/seattle-news/fbi-created-fake-seattle-times-web-page-to-nab-bomb-threat-suspect/ (last accessed Jan. 28, 2020).

[16] Special Agent Norman Sanders' Affidavit Seeking Search Warrant Authorizing CIPAV, Western District Court of Washington (June 2007) (made available by Electric Frontier Foundation, fbi_cipav-08, 31, https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav) (last accessed Jan. 28, 2020).

NIT and CIPAV by using different identifying names, this is at most a distinction without a difference.

Recently, the FBI has been seeking warrants to implement "a Network Investigation Technique." *See United States v. Broy*, 209 F.Supp.3d 1045, 1049 (C.D. Ill. Sept. 21, 2016). This does not mean, however, that the specific malware itself is called NIT—it is simply the moniker the FBI has used when they want to install malware on a suspect's computer. And since the government has refused to release the details of the malware used in these cases, courts have simply adopted the term. This is the same exact approach the government has taken with cell site simulators, by now simply referring to them as digital analyzers.

The actual malware used in the NIT cases very well could be CIPAV or a variation of malware which exploits different vulnerabilities yet produces the same identifying data. For example, in the CIPAV affidavit that ultimately identified the bomb threat suspect, the FBI indicated that they have different variations of the CIPAV.[17] NIT and CIPAV also obtain the same identifying information, and the warrants and affidavits used in both contain parallel language about how the malware operates.[18] Cybersecurity experts and journalists also believed that CIPAV

[17] *See* Special Agent Norman Sanders' Affidavit Seeking Search Warrant Authorizing CIPAV, Western District Court of Washington (June 2007) (made available by Electric Frontier Foundation, fbi_cipav-08, 31, https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav) ("Because the FBI cannot predict whether any particular formulation of a CIPAV to be used will cause a person(s) controlling the activating computer to activate a CIPAV, I request that this Court authorize the FBI to use multiple CIPAV's in conjunction with the target Myspace Account within 10 days of this Court authorizing the use of the first CIPAV.") (last accessed Jan. 28, 2020).

[18] For example, the NIT warrants and CIPAV affidavits define the user's computer that receives the malware as the "activating computer" and the malware is "designed" to "cause" the activating

may have been used in the Freedom Hosting hidden service operation on the Tor Network.[19] Frankly, CIPAV is used on a regular basis—one federal agent complaining that, "we are seeing indications that [CIPAV] is being used needlessly by some agencies, unnecessarily raising difficult legal questions (and a risk of suppression without any countervailing benefit.)" [20]

And much like with the QPS/DIA in the matter at hand, the FBI has provided support to other foreign government in an effort to help them use this malware. For example, in 2007, the German government sent an inquiry "asking about CIPAV" to the FBI.[21]

III. Governmental Use of the Galileo Remote Control System

Since at least 2014, the government has been using the Galileo Remote Control System ("RCS"), an invasive software engineered by the HackingTeam. The HackingTeam is an international software company that sells spyware to government agencies across the world.[22] Essentially, the RCS allows government agencies to

computer to "transmit data" which the government can use to identify the user by subpoenaing ISPs with the data.

[19] Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired, (Sept. 13, 2013), https://www.wired.com/2013/09/freedom-hosting-fbi/ (last accessed Jan. 28, 2020).

[20] *See* Email exchange between FBI agents (names redacted) (Mar. 7, 2002) (made available by Electric Frontier Foundation, fbi_cipav-05, 1, https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav) (last accessed Jan. 28, 2020).

[21] *See* Email exchange between FBI agents (names redacted) (Jul. 24, 2007) (made available by Electric Frontier Foundation, fbi_cipav-08, 9, https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav) (last accessed Jan. 28, 2020).

[22] Hacking Team, WikiPedia, *available at* https://en.wikipedia.org/wiki/Hacking_Team (last accessed Feb. 1, 2020)

infect a user's computer with malware by, for example, downloading an executable file, visiting a website, or watching a video online. The malware that infiltrates the computer then allows the government to bypass the exit node of the Tor Browser and identify a target's IP address. With one click, the malware is deleted off the target's computer leaving no evidence that the computer was ever infected with malware.

In a 2014 email exchange between an FBI agent and a member of the HackingTeam's support staff, the FBI inquired as to whether the RCS could be used to identify the real IP address of a Tor Bundle user ("TBB").[23] A TBB user is one who uses the Tor Network in conjunction with the Tor Browser. The email inquired into the ability of the RCS software to identify a specific user, as the FBI agent was only then able to obtain the IP address of the Tor exit node.[24] In response, the HackingTeam simply stated, "if he is using TBB you will get the real IP address of the target."[25]

The RCS allows government agencies to neutralize and decrypt the dark web.[26] As explained in its user manual:

[23] Charlie Osborne, *FBI Used HackingTeam Services To Unmask Tor User*, Zero Day (Jul. 15, 2015) https://www.zdnet.com/article/fbi-used-hacking-team-services-to-unmask-tor-user/ (last accessed Feb 1. 2020).

[24] Email From FBI Agent John Solano to HackingTeam Support, (Sep. 10, 2014) (made available by WikiLeaks, HackingTeam Archive, Email-ID 636440, https://wikileaks.org/hackingteam/emails/emailid/636440) (last accessed Feb 1. 2020).

[25] Email From HackingTeam Support Staff, Alberto Ornaghi, (Sep. 10, 2014) (made available by WikiLeaks, HackingTeam Archive, Email-ID 640672, https://wikileaks.org/hackingteam/emails/emailid/640672) (last accessed Feb 1. 2020).

[26] Lorenzo Franceschi-Biccierai, *Hacking Team Founder: Hey FBI, We Can Help You Crack the Dark Web*, Wired (Jun. 2, 2015), https://www.vice.com/en_us/article/8qxj4b/hacking-team-founder-hey-fbi-we-can-help-you-crack-the-dark-web (last accessed Feb. 1, 2020) ("the right technology to accomplish this exists, the right technology. . .to fight terrorist in cyberspace exists and is available now.").

> "In modern digital communications encryption is widely employed to protect users from eavesdropping. Unfortunately, encryption also prevents law enforcement and intelligence agencies from monitoring and preventing crimes and threats to the Nation's security. Remote Control System is the stealth, active interception solution tool that hides itself inside the target devices and enables active data monitoring and process control. Remote Control System is design to meet the higher expectations of the worldwide intelligence community."[27]

The RCS works by using what they refer to as "Agents" and "Collectors" to collect the information from the targeted device. The Agent is a software component that infects the targeted device, extracts information, and monitors the user's activity once it infects the device.[28] The Agent then sends back the extracted information to the Collector, which is essentially a hosting server.[29] The Agent uses the "Internet to contact the Collector; hence you control your targets regardless of where they are located."[30]

Basically, the Agent is the malware that is installed on a target's computer. "Once the target it identified,[31] the operator infects the target by taking advantage of the following events, common during internet usage: download an executable file

[27] *See* Remote Control System Galileo: The Hacking Suit For Governmental Interception, The HackingTeam, (made available by WikiLeaks at https://wikileaks.org/hackingteam/emails/fileid/47956/21998) (last accessed Feb 1. 2020).

[28] *Id.* at 9.

[29] *Id.* at 6.

[30] *Id.*

[31] This not mean that the user or device has actually been identified, just that the government has identified potential targets. For example, the IP address of the computer or device does not need to be identified before the device becomes infect. The government can identify their targets by figuring out what websites they visit, uploading the Agent to that website, and infect the device with malware.

(.exe); visits a website; watches a YouTube video; visiting a Web resource (e.g., pdf, docs)."[32] Following the Agent's extraction of information from a target's computer, the Agent can be uninstalled remotely "with a simple click. Once removed, the Agent and all its data are permanently deleted from the target device. You can configure the Agent to securely wipe all files, to resist to forensic analysis."[33] "Additional features are available to ease the infection process, such as…replace a legitimate web page with a custom one, for example to obtain login credentials or personal information."[34]

Had the government and QPS/DIA, in this matter, employed a similar software to obtained Mr. Mitrovich's alleged IP address, the use of a forensic expert would be fruitless, as any traces of malware would have already been wiped from his seized computer. Compelling the government to disclose the software and source code used in this investigation would be the only means for Mr. Mitrovich to find out if his Fourth Amendment rights were violated.

IV. The Use of Malware is a Fourth Amendment Search and Requires a Warrant

District courts addressing NIT-type software have held that the government engaged in a Fourth Amendment search of a user's computer by using malware to obtain the identifying information. *See United States v. Broy*, 209 F.Supp.3d 1045, 1054 (C.D. Ill. Sept. 21, 2016) (Because the defendant had a reasonable expectation

[32] *Id.* at 11.

[33] *Id.* at 12.

[34] *Id.* at 11.

in the privacy computer, "the use of the NIT constituted a Fourth Amendment search."); see *also United States v. Owens* 2016 WL 7053195, at *5, n.1 (E.D. Wis. Dec. 5, 2016) ("Various district courts have already addressed the issue in relation to the Specific NIT warrant in this case. The Court agrees with the majority of courts finding a Fourth Amendment search occurred." *Citing Broy*, 2016 WL 5172853, at *6; *United States v. Ryan Anthony Adams*, 2016 WL 421079, at *4 (M.D. Fla. Aug. 10, 2016); *United States v. Darby*, 190 F.Supp.3d 520, 530 (E.D. Vir. Jun. 3, 2016)). Using the *Katz v. United States* reasonable expectation of privacy analysis, courts have determined that a person has a reasonable expectation of privacy in his computer.[35] *See generally*, 389 U.S. 347 (1967). The courts also rely heavily on *Riley v. California*. 573 U.S. 373 (2014). *Riley* found that a person has a reasonable expectation of privacy in his phone and law enforcement needed a warrant to search the digital information on the phone. 573 U.S. at 386-88.

Riley rejected the argument that law enforcement did not need a search warrant to look through a cell phone's call log because a person does not have a reasonable expectation of privacy in that information which is voluntarily disclosed to third parties and obtainable by a pen register order. *Id.* at 400. The *Riley* court unanimously dismissed this argument holding that there was "no dispute" that the officer engaged in a Fourth Amendment search. *Id.* It was irrelevant that person may

[35] It should be noted that while most of the courts found that NIT engaged in a search, most of the defendants argued that a warrant that was obtained was defective because a magistrate judge violated the jurisdictional requirements of Rule 41. These arguments are no longer valid, however, because Congress changed the jurisdictional requirements after the cases were decided.

not have an expectation of privacy in some of the contents of the phone because a person has an expectation in the phone more broadly. Phones, like Mr. Mitrovich's computer, contain "a digital record of nearly every aspect" of a person's life and a person has a reasonable expectation of privacy in the device. *Id.* at 395-96.[36] Moreover, the Court found that even the call logs might contain more than just phone number voluntarily disclosed when a call is placed, they may include "identifying information" that an individual might add. *Id.* at 400.

The NIT courts relied on this reasoning to find that deploying NIT infringes on one's reasonable expectation of privacy in their computer, implicating the Fourth Amendment. *See United States v. Darby*, 190 F.Supp.3d 520, 530 (E.D. Vir. Jun. 3, 2016).[37] If malware was used on Mr. Mitrovich's computer to either identify his IP address or force his computer to exit the Tor Browser and enter an open internet connection, his Fourth Amendment rights was violated. *See United States v. Broy*, 209 F.Supp.3d 1045, 1053 (C.D. Ill. Sept. 21, 2016) (While the defendant did not have a reasonable expectation in some of the types of information that was seized, the defendant "had a reasonable expectation of privacy in his computer more generally

[36] The *Riley* Court referred to cellular phones as "minicomputers", implying that a person would have a greater expectation of privacy in a computer and its contents. *Id.* at 394.

[37] "Likewise, if an individual has a reasonable expectation of privacy in the contents of his or her personal computer, as he or she does, any the deployments of the NIT invades on that privacy, then the NIT is a search. The NIT in this case caused Defendant's computer to download certain code without the authorization or knowledge of Defendant. The "contents" of a computer are nothing but its code. In placing code on Defendant's computer, the government literally—one writes code—invaded the contents of the computer. Additionally, the code placed on Defendant's computer caused Defendant's computer to transmit certain information without the authority or knowledge of Defendant. In this manner the government seized the contents of Defendant's computer. Just as in *Riley*, it is irrelevant that Defendant might not have a reasonable expectation of privacy in some of the information searched and seized by the government. The government's deployment of the NIT was a Fourth Amendment search." *Id.* at 530.

under *Riley*. Thus the use of the NIT constituted a Fourth Amendment search."); *see also United States v. Adams*, 2016 WL 4212076, at *4 (M.D. Fla. Aug. 10, 2016) ("For example, a defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage.").

Even if the government maintains that malware was not deployed into Mr. Mitrovich's computer, which is highly unlikely given that links to open internet website open and operate within the Tor Browser, they still must be compelled to disclose the source code because regardless of how the hyperlink operated, it still forced Mr. Mitrovich's computer to disclose its information when the "video file. . .*captured and recorded* the user's true IP address." Dkt. No. 53, pg. 2 (emphasis provided). As a Michigan District recently found in a Playpen related matter, "[i]f a user who has taken special precautions to hide his IP address does not suffer a Fourth Amendment violation when a law enforcement officer compels his computer to disclose his IP address…and other identifying information, then it is difficult to imagine *any* kind of online activity which is protected by the Fourth Amendment." *United States v. Kahler*, 236 F.Supp.3d 1009, 1021 (E.D. Mich. Feb. 14, 2017) (emphasis provided). The court noted that "internet use pervades modern life" before holding that "law enforcement, acting alone, may not compel the computers of internet users into revealing identifying information without a warrant, at least when the user has taken affirmative steps to ensure that third parties do not have that information." *Id.* The "affirmative steps" that the court referred to was using the Tor Network and Tor Browser.

V. The Acquisition of Mr. Mitrovic's IP Address Was a Search Under a Property-Based Approach to the Fourth Amendment

Under a property-based theory of the Fourth Amendment, Mr. Mitrovich's IP address constitutes his "papers and effects," regardless of whether it was shared with a third-party, such as the first "node" computer in the Tor Network. It, therefore, cannot be searched or seized without a valid warrant. *Carpenter v. United States*, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J., dissenting).

In his dissenting opinion in *Carpenter*, Justice Gorsuch opined that under a "traditional approach" to the Fourth Amendment, the protection against unreasonable searches and seizures applied as long as "a house, paper or effect was yours under law." *Id.* Justice Gorsuch drew a strong analogy between cell phone location data and mailed letters, in which people have had an established Fourth Amendment property interest for over a century, whether or not these letters are held by the post office. *Id.* at 2269; *citing Ex party Jackson*, 96 U.S. 727, 733 (1877)).

Here, Mr. Mitrovich's alleged IP address belongs to him. He may have shared his IP address with the first Tor "node" computer, but he simply entrusted it with the information, as many people do with other websites such as Google. This does not mean he forfeited his Fourth Amendment interests in it.

As Justice Gorsuch explained in *Carpenter*, "[e]ntrusting your stuff to others is bailment. A bailment is the 'delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.'" 138 S. Ct. at 2268-69 (Gorsuch, J., dissenting). Here, the Tor "node" is the bailee, and it owes a duty to the bailor, Mr. Mitrovich, to keep his data safe. In other words, Mr. Mitrovich retains the right to exclude others from his IP address, a quintessential feature of property ownership. *See* William Blackstone, 2 Commentaries on the Law of England *2 (1771) (defining property as "that sole and despotic dominion . . .exercise[d] over the external things. . .in total exclusion of the right of any other."); *Loretto v. Teleprompter Manhattan CATV Corp*., 458 U.S. 419, 435 (1982) (calling the right to exclude "one of the most reassured strands" of the property rights bundle); *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (19799) (calling the right to exclude "one of the most essential sticks" in the property rights bundle).

The government eviscerated Mr. Mitrovich's right to exclude others from this IP address. This trespass constitutes a Fourth Amendment search and seizure, no less than a violation of one's "reasonable expectation of privacy."

Conclusion

Wherefore, for the aforementioned reasons, Mr. Mitrovich respectfully requests this Honorable Court to grant his Motion to Compel and order the government to disclosed the requested discovery. The embedded hyperlink employed in the TLZ sting must have contained malware that trespassed Mr. Mitrovich's computer. The government's theory that a video on the open internet revealed the identifying information, or that Mr. Mitrovich was not invasively redirected to the open internet, is simply implausible and inconsistent with how Tor operates. This investigation, on its face, transpired in almost the exact same manner as the previous watering hole stings, and there is a good-faith basis to believe that the hyperlink link contained a CIPAV-like malware, if not CIPAV itself. The sought-after discovery is needed to ensure Mr. Mitrovich's Fourth Amendment rights are protected.

Respectfully submitted,

/s Vadim A. Glozman
Attorney For The Defendant

Vadim A. Glozman
VADIM A. GLOZMAN LTD.
Attorney at Law
53 W. Jackson Blvd., Suite 1410
Chicago, IL 60604
(312) 726-9015

CERTIFICATE OF SERVICE

I, Vadim A. Glozman, an attorney for Defendant Deny Mitrovich, hereby certify that on this, the 1st day of February, 2020, I filed the above-described document on the CM-ECF system of the United States District Court for the Northern District of Illinois, which constitutes service of the same.

Respectfully submitted,

*/s/ Vadim A. Glozman*____

Vadim A. Glozman
VADIM A. GLOZMAN LTD.
53 W. Jackson Blvd., Suite 1410
Chicago, IL 60604
(312) 726-9015